EX PARTE OR LATE FILED

PRIVACY

Safeguarding Telecommunications-Related Personal Information

CC Docket No. 96-115

U.S. DEPARTMENT OF COMMERCE
National Telecommunications and Information Administration

PRIVACY AND THE NII:

Safeguarding Telecommunications-Related Personal Information

U.S. DEPARTMENT OF COMMERCE
Ronald H. Brown, Secretary
David J. Barram, Deputy Secretary
Larry Irving, Assistant Secretary and
Administrator, National Telecommunications
and Information Administration
Washington D.C.

October 1995
[First Reprint]

Assistant Secretary for Communications and Information and Administrator, National Telecommunications and Information Administration

Larry Irving

Acting Deputy Assistant Secretary, Deputy Administrator

Michele C. Farquhar

Office of Policy Analysis and Development, Associate Administrator

Kathryn C. Brown

PROJECT TEAM

Jerry Kang[1]
Radhika Karmarkar[2]
Lisa Leidig

Project Contributors

Office of Policy Analysis and Development

Joseph L. Gattuso
Alfred M. Lee
Tim Sloan

Lavern James
(cover design)

Mary Stewart
(support staff)

Office of the Chief Counsel

Barbara Wellbery
Chief Counsel

Timothy Robinson
Cathleen Kelly
Cheryl Kinsey

Office of International Affairs

Cynthia Rich

Acknowledgements

We wish to thank Carol E. Mattey, now Deputy Chief of the FCC Common Carrier Bureau's Policy and Program Planning Division, for her substantial role, while at NTIA, in the preparation of NTIA's Privacy Notice of Inquiry. We wish to thank Michael Francesconi, Jim McConnaughey, Joanne Kumekawa, Sallianne Fortunato, and David Gardner for their assistance in reviewing drafts of this report and for their helpful comments and suggestions. We also wish to thank Arthur J. Altenburg for his document layout and typesetting support.

---

1 Currently Acting Professor, UCLA School of Law.

2 Currently Attorney-Adviser, FCC Common Carrier Bureau, Policy and Program Planning Division.

EXECUTIVE SUMMARY

As the National Information Infrastructure (NII) is built, more and more individuals will use it for a wide range of transactions. In the course of using the NII, individuals will create information trails that could provide others, in the absence of safeguards, with the personal details of their lives.

In this White Paper, the National Telecommunications and Information Adminstration (NTIA) hopes to contribute to the broader privacy debate by addressing the privacy issues related to a specific sector -- the telecommunications sector. Specifically, this paper focuses on the privacy concerns associated with an individual's subscription to or use of a telecommunications or information service. The overall purpose of the paper is to provide an analysis of the state of privacy in the United States as it relates to existing and future communications services and to recommend a framework for safeguarding telecommunications-related personal information (TRPI).

The analysis provided herein reveals that there is a lack of uniformity among existing privacy laws and regulations for telephony and video services. In fact, similar services are governed differently depending on how they are delivered. And, other communications services like those available over the Internet are almost entirely unprotected. Furthermore, NTIA believes that it will become increasingly difficult to apply existing privacy laws and regulations to communications service providers as services and sectors converge, and as new technologies evolve.

To rectify limitations in existing telecommunications privacy law and to provide consumers with a uniform privacy standard for TRPI, NTIA proposes a framework that draws upon the Information Infrastructure Task Force's *NII Principles for Providing and Using Personal Information*. This framework has two fundamental elements -- provider notice and customer consent.

Under this proposed framework, telecommunications and information service providers would notify individuals about their information practices, abide by those practices, and keep customers informed of subsequent changes to such practices. Service providers would be free to use information collected for stated purposes once they obtain consent from the relevant customer. Affirmative consent would be required with respect to sensitive personal information. Tacit customer consent would be sufficient to authorize the firm to use all other information.

NTIA believes that establishing minimum privacy protections across the communications industry would ensure that consumers are provided with a reasonable level of privacy protection. Uniformly applied, a common "base" standard could also prevent some industries from gaining an unfair competitive advantage.

Table of Contents

PRIVACY AND THE NII

The real danger is the gradual erosion of individual liberties through the automation, integration, and interconnection of many small, separate record-keeping systems, each of which alone may seem innocuous, even benevolent, and wholly justifiable.

U.S. Privacy Protection Study Commission[1]

The numbers dialed from a private telephone—although certainly more prosaic than the conversation itself—are not without "content." Most private telephone subscribers may have their own numbers listed in a publicly distributed directory, but I doubt there are any who would be happy to have broadcast to the world a list of the local or long distance numbers they have called. This is not because such a list might in some sense be incriminating, but because it easily could reveal the identities of the persons and the places called, and thus reveal the most intimate details of a person's life.

Supreme Court Justice Potter Stewart

Smith v. Maryland [2]

I. INTRODUCTION

An advanced national information infrastructure (NII) promises enormous economic, social, and cultural benefits to its users and to the nation—enhanced educational and employment opportunities for all Americans, greater citizen participation, and improved delivery of government services. The NII can produce these benefits because it will facilitate and expand the flow of information from people to people and from place to place.[3] However, many people

1 World Wide Web Computer Home Page of Privacy Rights Clearinghouse, http://www.manymedia.com/prc (quoting U.S. Privacy Protection Study Commission, 1977).

2 *Smith v. Maryland*, 442 U.S. 735, 748 (1979) (Stewart, J., dissenting).

3 The Clinton Administration envisions the NII as "a seamless web of communications networks, computers, databases, and consumer electronics that will put vast amounts of information at users' fingertips." Information Infrastructure Task Force, U.S. Dep't of Commerce, *The National Information Infrastructure: Agenda for Action*, 58 Fed. Reg. 49,025 (1993) [hereinafter *Agenda for Action*]. Many of the individual components of this "network of networks" are in place already, and U.S. companies are investing more than $50 billion annually to upgrade existing facilities and to construct new ones. The Administration's NII Initiative seeks to develop policies and programs to spur the evolution of the existing infrastructure into a network of networks. *See* National Telecommunications and Information Administration, *Inquiry on Privacy Issues Relating to Private Sector Use of Telecommunications-Related Personal Information*, 59 Fed. Reg. 6842, 6842 n.5 (1994) [hereinafter *Privacy NOI*].

may be reluctant to use the NII if they are afraid that the personal information transmitted over it can be used in ways that are unexpected or inappropriate. Thus, if government and the private sector want to encourage the vigorous consumer activity needed to unlock the full potential of the information infrastructure, they must acknowledge and safeguard the legitimate privacy interests of NII users.

A. The Nature of Privacy

More than sixty years ago, Supreme Court Justice Louis Brandeis characterized the right to privacy—"the right to be let alone [as] the most comprehensive of rights, and the right most valued by civilized men."[4] A 1993 public opinion survey by Louis Harris & Associates found that 83% of Americans are concerned about threats to personal privacy.[5] This reflects a five point increase over responses to the identical question posed a year earlier, and a 49 point increase from a similar poll conducted in 1970.[6] In addition, a survey of members of the U.S. Chamber of Commerce revealed "a staggering 59.2% . . . stat[ing] that they view the emerging issue of privacy in telecommunications as very important; 34.8% felt it was moderately important."[7] Furthermore, the Privacy Rights Clearinghouse (PRC) reports that consumers are "frustrated by a lack of control they have over the use of their personal information;" and "suffer" from a lack of understanding about how information about them is collected, used, and distributed and from a "misunderstanding" of existing privacy protection laws and regulations.[8]

"Privacy" means different things depending on the context.[9] Among the many notions of privacy, growth of the NII primarily raises concerns about *information privacy*. That term refers to an individual's claim to control the terms under which "personal information"—information

---

4 *Olmstead v. United States*, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).

5 *Privacy NOI, supra* note 3, at 6842 n.6 (citing *Public's Privacy Concerns Still Rising*, Privacy & Am. Bus., Sept./Oct. 1993, at 3).

6 *See* Larry Tye, *Proposed "Bill of Rights" Would Limit Personal Data*, Boston Globe, Sept. 8, 1993, at 6 (electronic version).

7 Letter from Fred H. Williamson, Chairman, Telecommunications Infrastructure Task Force, U.S. Chamber of Commerce, to the National Telecommunications and Information Administration (July 12, 1994) (On file at NTIA).

8 Privacy Rights Clearinghouse, *First Annual Report of Privacy Rights Clearinghouse* 11-14 (Center for Public Interest Law, University of San Diego) (Jan. 1994).

9 Even a partial list of these ideas includes such disparate concepts as: the privacy of private property; privacy as a proprietary interest in name and image; privacy as the keeping of one's affairs to oneself; the privacy of internal affairs of a voluntary association or of a business; privacy as the physical absence of others who are unqualified by kinship, affection, or other attributes to be present; respect for privacy as the respect for the desire of another person not to disclose or to have disclosed information about what he is doing or has done; the privacy of sexual and familial affairs; the desire for privacy as the desire not to be observed by another person or persons; and the privacy of the private citizen as opposed to the public official. U.S. Congress, Office of Technology Assessment, OTA-TCT-606, *Information Security and Privacy in Network Environments* 82 (Sept. 1994) (quoting Edward Shils).

that can be linked to an individual or distinct group of individuals (*e.g.*, a household)[10]—is acquired, disclosed, and used.[11]

Information privacy promotes two principal interests. It recognizes that control over personal information is important because mere awareness by others of certain types of information is potentially harmful. For example, an individual may want to keep certain types of health data confidential from the general public because its disclosure could cause the person embarrassment. Information privacy also recognizes that personal information can be used improperly, unfairly, or for purposes other than those intended by an individual. For example, an individual may refuse to disclose his or her social security number or mother's maiden name, not because disclosure in itself would be harmful but because that information could be used to gain telephone access to banking records.[12]

Concerns about safeguarding privacy will likely grow as the NII becomes a pervasive, functioning reality.[13] As the NII is built, more and more individuals will use it to execute an ever-expanding range of transactions involving, for example, business, entertainment, banking, education, recreation, and even health care. These transactions—by their very execution on the NII—create electronic records, which are easily stored and processed.[14]

---

10 Personal information also includes information that is not personally identifiable on its face, but identifiable in context. In contrast, aggregate information about society as a whole—its average age, income, or ethnic characteristics; its television viewing habits; its consumption patterns—does not implicate the reasonable privacy interests of any of its members.

11 *See* Information Infrastructure Task Force, Privacy Working Group, *Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information*, Commentary ¶2, (June 1995) [hereinafter *IITF Principles]*. Similar definitions of information privacy appear in the literature. *See, e.g.*, Alan F. Westin, *Privacy and Freedom* 7 (1966) ("Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."); W.A. Parent, *Recent Work on the Concept of Privacy*, 20 Am. Phil. Q. 341, 346 (1983) (Privacy is "the condition of a person's not having undocumented personal information about himself known by others."); Advisory Committee on Automated Personal Data Systems, U.S. Dep't of Health, Education & Welfare, DHEW Pub. No. (OS) 73-94, *Records, Computers, and the Rights of Citizens* at xx (July 1973) [hereinafter *DHEW Principles]* ("Concern about computer-based record keeping usually centers on its implications for personal privacy, and understandably so if privacy is considered to entail control by an individual over the uses made of information about him.").

12 *See generally* Privacy Rights Clearinghouse, *Second Annual Report* 28-32 (1995).

13 Such concerns will also be present with respect to a "Global Information Infrastructure," or GII, and these issues are already being addressed in other parts of the world. For example, the European Union has adopted a directive "on the protection of individuals with regard to the processing of personal data and on the free movement of such data. The European Parliament and the Council of the European Union, *Directive of the European Parliament and of the Council on the Protection of Individuals With Regard to the Processing of Personal Data and on the Free Movement of Such Data*, (Directive 95, 12003/4/94 REV 4) (Brussels 1995).

14 For example, by following a users' mouse-click patterns and trails over the Internet, direct marketers can improve their ability to target users interested in a specific product. *See* Andy Kessler, *Tracking Mouse Droppings*, Forbes ASAP, Aug. 28, 1995, at 67.

Further, because the costs associated with storing, processing, and distributing personal records are continuously decreasing, accumulating personal information from disparate sources will become a cost-effective enterprise for information users with interests ranging from law enforcement to direct marketing.[15] For example, in one case, journalists spent an average of $112 and 75 minutes on-line to find financial, legal, marital, and residential histories of various luminaries, such as movie producer George Lucas and White House Chief of Staff Leon Panetta.[16] Finally, entirely new modes of communication and transactions may be created that are not contemplated by current privacy regulations and policies,[17] which are typically tied to today's or even yesterday's technologies. For instance, interactive, switched, broadband communications networks, which will enable individuals to educate and entertain themselves, to shop, to receive health care, to bank, and to participate in government over a single network, could pose new privacy concerns. In the absence of subscriber privacy provisions appropriate to such networks and technologies, it will be possible for others to track and store information about the daily activities of one's life.

B. NTIA's Inquiry

These developments presage an information environment in which more personal information will flow more quickly, more widely, more invisibly, and more cheaply with fewer legal and social constraints. To understand better the privacy issues implicated by that environment, the National Telecommunications and Information Administration (NTIA)[18] released a Notice of Inquiry[19] on private sector use of telecommunications-related personal

---

Several on-line companies already track and sell information derived from "mouse droppings." For instance, Internet Profiles Corp. in San Francisco uses its software to track who visits a particular Web site, what is looked at and for how long. This company sells this information to the relevant Web site operator for $5,000 per report. John W. Verity, *Bites & Bytes: Market Data for Online Advertisers*, Bus. Wk. Aug. 28, 1995, at 72.

15 Appendix A discusses privacy issues related to marketing profiles, which are records of an individual's characteristics created by accessing personal information from various sources and matching that information to a particular individual. The Appendix focuses on how merchandisers and national list-compilers acquire and process TRPI to create profiles to market products and services.

16 *See* Charles Piller, *Privacy in Peril*, MacWorld, July 1993, at 12.

17 *See infra* text at Part II (discussing these privacy protections).

18 NTIA, a part of the U.S. Department of Commerce, is the Executive Branch agency principally responsible for developing and articulating domestic and international telecommunications and information policies. As the principal adviser to the President on these policies, NTIA conducts studies and makes recommendations regarding telecommunications policies, activities, and opportunities, and presents Executive Branch views on telecommunications matters to the Congress, the Federal Communications Commission (FCC), state and local governments, and the public. NTIA was established by Executive Order in 1976. Exec. Order No. 12,046, 3 C.F.R. (1978), *reprinted as amended in* 47 U.S.C. § 305 note (1988). Congress codified NTIA's functions in the National Telecommunications and Information Administration Organization Act of 1992, 47 U.S.C. §§ 901-927 (Supp. V 1993).

19 *Privacy NOI, supra* note 3.

information.[20] We received 46 formal comments from industry, the press, academics, privacy advocates, and individuals.[21] These comments, supplemented by consultations with stakeholders in the privacy debate, feedback from experts, and independent research, form the basis of this report. NTIA hopes that this White Paper will serve as a catalyst, inspiring industry and consumer advocates to work together to instill the consumer confidence essential for the viability of the NII.

C. Scope of the White Paper

As the President's adviser on telecommunications and information policy, NTIA in this paper will focus on private sector collection, use, and dissemination of telecommunications-related personal information (TRPI)—personal information that is created in the course of an individual's subscription to a telecommunications or information service or as a result of his or her use of that service.[22] To illustrate the concept of TRPI, consider an electronic mail service that allows individuals to log on to the service via modem and send e-mail messages through the

---

20 Without question, equally important issues regarding governmental use of personal information exist, but those issues have been discussed and analyzed elsewhere. *See, e.g.*, The Privacy Protection Study Commission, *Personal Privacy in an Information Society* 345-91 (1977). By contrast, relatively little attention has been paid to the private sector's use of personal information. Partly due to decreasing costs of information processing, the private sector has come to rival the government in acquiring and using personal information. *See, e.g.*, John Markoff, *Remember Big Brother? Now He's a Company Man*, N.Y. Times, Mar. 31, 1991, at E7, ("[N]ow many computer professionals and civil liberties specialists say they fear that if a Big Brother finally arrives he may be wearing not a police uniform but a business suit."). In fact, recent polls indicate that the American public is concerned about threats to privacy from the private sector as much as from government. *See* Anne Wells Branscomb, *Who Owns Information?: From Privacy to Public Access* 17 (1994).

21 The 46 included six local exchange carriers (LECs), three interexchange carriers, 11 information service providers and associations representing information service providers, 13 private citizens, seven public interest groups, two state public utility commissions, the American Bankers Association, the United States Council for International Business, the Independent Data Communications Manufacturers Association, and the National Cable Television Association. For convenience, all subsequent citations to "Comments" shall refer to papers filed in response to NTIA's Privacy NOI.

22 This paper does not address privacy issues related to the contents of a communication. Content data is the content of a communication between two parties. It is information, typically authored or prepared by one party, and sent to another party. By contrast, transactional data is information created in the course of transmitting content data. Although privacy of content data raises important questions, these questions have been examined, principally in the debate over law enforcement's ability to intercept digital and encrypted communications. *See generally* U.S. Congress, Office of Technology Assessment OTA-TCT-606, *Information Security and Privacy in Network Environments* (Sept. 1994); U.S. Congress, Office of Technology Assessment OTA-BP-ITC-147, *Issue Update on Information Security and Privacy in Networked Environments* (June 1995). Less understood is how privacy may be threatened not by disclosing a communication's contents but by collecting information about how individuals will use the NII.

At times, the difference between transactional data and content data may be meaningless. Consider a movie delivered through a cable system. In some sense, the content data is the signal carried through the cable and deciphered into video frames displayed on the television. But from a privacy perspective, there is no difference between this data and the transactional data that identifies the title of the movie.

Internet.[23] To subscribe to this service, the provider will typically collect some basic information about the customer, such as name, home address, home telephone number, work telephone number, type of e-mail service requested, and credit card (or other payment) information. Once the e-mail service has been installed, additional data will be generated each time the customer sends an e-mail message. That includes all the personal information created in the course of routing a message from the individual to the addressee (*e.g.*, header information on an e-mail message), as well as certain accounting information, which, depending on how the service charges its customers, could include the date, time, subject line of message, and its length. All of this subscription and usage data constitutes TRPI.

Although most consumers are probably aware that telecommunications and information service providers collect a wide range of subscription data, they may be less aware of providers' accumulation of other TRPI and the uses to which that data can be put. Many consumers may have the same level of awareness as the woman who told a caller trying to sell long distance service that she did not make many out-of-town calls:

> *"I'm surprised to hear you say that," she recalls him saying. "I see from your phone records that you frequently call Newark, Delaware, and Stamford, Conn." . . . "I was shocked, scared, and paranoid," she recalls. "If people are able to find out who I call, what else could they find out about me?"*[24]

The risks for consumers will likely increase in the future as several related factors induce providers of telecommunications and information services to become more sophisticated and aggressive in their use of TRPI. First, the continuing growth of competition in those markets will increase the number of firms competing for consumer attention. In that environment, companies like the enterprising long distance service provider in the foregoing anecdote will find TRPI a powerful resource for identifying potential customers and tailoring the companies' marketing strategies to maximize customer response.

Second, as established service providers diversify into other lines of business, their existing reservoir of TRPI will help them sell those new services more effectively and at less cost. Thus, when MCI and Rupert Murdoch's News Corp. announced a joint venture to market on-line information services, MCI executives said that they would use TRPI in their "Friends and Family" database to offer these services to some of MCI's current long distance customers.[25]

Third, as competition continues to squeeze profit margins, more and more telecommunications and information service providers may come to view the sale of TRPI as an additional,

---

23 The Internet is an outgrowth of U.S. government-supported research and development in networking. It connects millions of computers and users in over 160 countries. People use the Internet to exchange e-mail, browse through digital libraries, publish multimedia documents, conduct electronic commerce, participate in video-conferences, and engage in a variety of social activities. *See generally* Ed Krol, *The Whole Internet Users Guide and Catalog* (2d ed. 1994).

24 Jeffrey Rothfeder, *Is Nothing Private?*, Bus. Wk., Sept. 4, 1989, at 74.

25 John M. Higgins, *Benefits Hazy for MCI's Murdoch deal*, Multichannel News, May 15, 1995, at 2.

low-cost revenue stream. However, it is not clear to what extent consumers will accept such practices. For example, although companies have long made a practice of extracting information from local phone books and selling it to marketers, when telephone companies have announced their intent to sell customer listings, they have been met with opposition. In 1990, New York Telephone informed its customers through billing statements about its plans to sell customer listings, and 800,000 customers asked to have their names removed from the lists.[26] Bell Atlantic experienced a similar reaction when it announced plans to sell its "white pages" directory lists in July 1995.[27] Furthermore, in response to the public comments the Federal Communications Commission (FCC) received to its Notice of Proposed Rulemaking on Caller ID,[28] it passed rules prohibiting the sale or reuse of automatic number identification (ANI)-derived information without first notifying the originating telephone subscriber, and obtaining his or her affirmative consent for such reuse or sale.[29] ANI, a subset of TRPI, is a signaling protocol used by carriers to automatically identify a calling party's billing telephone number. Some states have adopted similar rules restricting the use of ANI.[30]

D. Recommended Approach

The coming years thus promise increasing tension between the desire of telecommunications and information service providers to expand the use of TRPI to market new services—many of which will doubtless benefit consumers—and consumers' desire to control the dissemination of potentially sensitive personal information. The relevant questions for policy makers are: what level of privacy protection adequately balances the legitimate interest of individuals and service providers; whether existing laws and regulations provide the desired level of protection; and, if not, what changes should be made.

---

26 New York Telephone withdrew its proposal to market its white pages directory database because of a high level of customer opposition. *See* Dottie Enrico, *Dollars and Dialers: Phone Company's Plan to Sell Names Stirs Controversy*, Newsday, June 11, 1990, at 3.

27 Bell Atlantic also withdrew its plans to sell directory listings to marketers. *See, e.g., Communications Daily*, July 25, 1995 (electronic version).

28 *See Rules and Policies Regarding Calling Number Identification Service*, Notice of Proposed Rulemaking, 6 FCC Rcd 6752 (1992).

Caller ID is a service that enables telephone subscribers to see a calling party's telephone number. As this paper addresses the commercial use of TRPI and Caller ID is primarily marketed to residential consumers, it does not examine the privacy issues related to Caller ID.

29 *See Rules and Policies Regarding Calling Number Identification Service - Caller ID*, Report and Order and Further Notice of Proposed Rulemaking, 9 FCC Rcd 1764 (1994). Order stayed *see Rules and Policies Regarding Calling Number Identification Service - Caller ID*, 10 FCC Rcd 4364 (1995).

Historically, local telephone companies have passed ANI on to long-distance carriers for routing and billing purposes. However, recently ANI has been passed on to third parties for marketing purposes.

30 For example, New York's Public Service Commission has also issued terms and conditions for how ANI is derived and disseminated to parties. *See* Comments of the State of New York, Dep't of Pub. Serv. at App. B.

The United States currently has no omnibus privacy law that covers the private sector's acquisition, disclosure, and use of TRPI. Instead, American privacy law comprises a welter of Federal and state statutes and regulations that regulate the collection and dissemination of different types of personal information in different ways, depending on how it is acquired, by whom, and how it will be used.[31] Although these laws provide some level of privacy protection, they are not comprehensive in the sense that they do not apply uniformly to all service providers.

As discussed more fully below, this is particularly true with respect to the principal regulations governing the acquisition and use of TRPI by certain providers of telecommunications and information services—the FCC's rules pertaining to telephone companies' use of customer proprietary network information (CPNI) and the provisions of the 1984 Cable Act regulating the disclosure of "personably identifiable" subscriber information by cable television operators.[32] Because those requirements were imposed on a limited group of service providers, they afford consumers little, if any, protection against inappropriate use of TRPI by other types of service providers. As importantly, the limited applicability of those regulations virtually guarantees that different firms will have differing privacy obligations even when they offer similar services, creating a situation that could be potentially disadvantageous to one competitor or group of competitors.

To rectify these limitations in existing telecommunications privacy law and to provide consumers with a uniform privacy standard, NTIA has applied the Information Infrastructure Task Force's (IITF)[33] *NII Principles for Providing and Using Personal Information* to the telecommunications sector in order to offer a framework for the acquisition and use of TRPI by telecommunications and information service providers. We hope that this recommendation will contribute to the broader debate regarding privacy concerns and the NII, assist the Administration's IITF, its Advisory Council,[34] the FCC, Congress, state and local governments, and private sector policy makers as they grapple with this important issue. NTIA also hopes that this application of the IITF's Principles will encourage other sectoral analyses.

As stated above, NTIA's proposed framework draws upon the IITF's Principles and has two fundamental elements—provider notice and customer consent. Under NTIA's proposed framework, each provider of telecommunications and information services would inform its customers about what TRPI it intends to collect and how that data will be used. A service

---

31 For a comprehensive review of U.S. privacy statutes, see Robert Smith, *Compilation of State & Federal Privacy Laws* (Privacy Journal 1992).

32 47 U.S.C. § 551 (1990). Personally identifiable subscriber information and CPNI are both subsets of TRPI.

33 The IITF is a Federal inter-agency group convened by President Clinton to "work with Congress and the private sector to propose the policies and initiatives needed to accelerate deployment" of the NII. *See Agenda for Action*, *supra* note 3, at 49,027.

34 The President created the NII Advisory Council (NIIAC) to advise the Secretary of Commerce, and the Administration, on a national strategy for promoting the development of the NII. The Council is comprised of individuals representing various interests including industry, labor, academia, public interest, and state and local governments. *See* Exec. Order No. 12,864, 58 Fed. Reg. 48,773 (1993).

provider would be free to use the information collected for the stated purposes once it has obtained consent from the relevant customer. Affirmative consent would be required with respect to sensitive personal information. Tacit customer consent would be sufficient to authorize the use of all other information.

This approach, if embraced by industry, would allow service providers and their customers to establish the specific level of privacy protection offered in a marketplace transaction, free from excessive government regulation, so long as the minimum requirements of notice and consent are satisfied. The uniformity contemplated by this approach means its adoption would not create competitive imbalances among rival firms, but would preserve their ability to compete on privacy as vigorously as they compete on price, service, and quality.[35] Further, because NTIA's recommended framework gives companies considerable flexibility in giving notice and securing consent, implementation of that approach should not be overly burdensome. On the other hand, this approach would reassure consumers that their reasonable privacy expectations will be respected when they use the NII. Uniformity across the communications sector should encourage more consumer use of the NII which, in turn, would create and expand market opportunities for information and to service providers of all types. For these reasons, NTIA believes that it is in the private sector's interest to adopt the privacy framework outlined in this paper, without waiting for formal government action.

II. CURRENT REGULATION OF TRPI

Communications providers play an absolutely critical role in transmitting information among transacting parties in our society. In the course of transmitting information, communications providers are privy to a wide variety of TRPI. For example, in providing long-distance telephone service, telephone companies generate calling records that identify the origination and destination telephone numbers, and the time and length of each phone call. Such information may be disclosed or used in ways inconsistent with an individual's expectation of privacy. In one prominent case involving two Florida Public Service Commission officials, a private investigator obtained a year's worth[36] of telephone calling records.[37] Although the officials were surprised to learn of the activities of the private investigator, a subsequent investigation confirmed that the disclosure by the telephone company was legal under state and Federal law.[38]

---

35 To a certain degree, AT&T is already competing with MCI on privacy. Whereas MCI uses information from its customers' "Friends & Family" portfolios to target new customers and present new services, AT&T advertises over national television that it does not.

36 *See* L. Morgan, *High Stakes Data Gathering Raises Query: How Far Is Too Far?*, St. Petersburg Times, Oct. 2, 1993, at 4B.

37 *See* B. Moss, *Release of Phone Records Was Legal, PSC Determines*, St. Petersburg Times, June 16, 1994, at 4B.

38 *See Investigation Into Dissemination of Long Distance Telephone and Other Customer Records and Related Customer Privacy Issues*, Florida Pub. Serv. Comm'n, Docket No. 931019-TP, Order No. PSC-94-0695-FOF-TP, 94 FPSC 6:92 (June 7, 1994).

While recognizing a growing variety of services in the communications marketplace, this discussion will focus on two particular communications services—telephony and video—as representative examples of how and what types of TRPI are routinely collected and of regulatory and statutory protections currently available for limiting the disclosure of TRPI. This review indicates that current legal norms have led to a patchwork of privacy protection that may lead to disparate treatment of different service providers even as they provide similar services. Already, technological advances and market deregulation are dissolving traditional distinctions between communications providers such as telephone companies and cable operators. Telephone companies are beginning to offer cable-like services; cable operators are beginning to offer telephony-like services; and companies are forming hybrid alliances to develop new advanced communications services.[39] With an increasing convergence among services and service providers, differences in the handling of TRPI may lead to competitive inequities and customer confusion, which may in turn hinder the deployment of new services and technologies.

A. TRPI Collected by Telephone and Video Service Providers

Telephone services—both local and long distance services—generate a wealth of TRPI. When a customer subscribes to a telephone service, TRPI in the form of subscription data is collected to initiate and secure the commercial relationship between the individual and the telephone service provider. Such data might include the subscriber's name and address; number and types of access lines (*e.g.*, residential or business) used; any chosen advanced services (*e.g.*, call handling features such as call waiting, caller ID, call forwarding, and anonymous call rejection); and choice of prescribed interexchange carrier.

With each phone call an individual makes, the telephone service provider collects TRPI in the form of transactional data. This includes routing data necessary to deliver the communicative content between the calling parties, as well as the accounting data necessary to bill the appropriate individuals. As noted above, for each call, this transactional data typically includes the originating phone number, destination phone number, and depending on the circumstances, the time and length of the call.

As Justice Stewart noted,[40] these calling records can reveal a great deal about the individual even without divulging the communicative contents of the phone call. With the help of a reverse-telephone directory, available in many libraries, one can easily identify the names and addresses

---

39 Telephone and cable companies are already teaming up to provide video programming, local, and long-distance telephone service over the same network. For example, Sprint has formed a joint-venture with TCI, Comcast Corp., and Cox Communications to offer local, long distance, and wireless phone service. Martin Rosenberg, *Sprint Cites Ambitious Goal; Boosted by Cable Alliance, it Aims to Add a Million Customers*, Kansas City Star, July 14, 1995, at B1. Time Warner and AT&T are considering forming a venture to sell a full range of phone services through Time Warner's cable system. John Keller, *Time Warner's Cable-TV Unit & AT&T in Talks*, Wall St. J., May 16, 1995, at A3. Also, cable companies and Internet Service Providers are making plans jointly to provide broadband access to the Internet. *See* Leland L. Johnson, *Toward Competition in Cable Television* 46 (1994).

40 *See Smith v. Maryland*, 442 U.S.735, 748 (Stewart, J., dissenting).

associated with the originating and destination phone numbers. Such information could reveal the identity of one's friends and colleagues, and the patterns of one's work and sleep.

Video service providers collect types of subscription data similar to that collected by telephone service providers. In addition to name, address, and telephone number, they typically will compile information concerning tiers of service or specific premium channels requested, carrying such programming as popular movies, children's shows, sports, or adult entertainment. Subscription data will also likely include the types of equipment necessary to initiate the video service, such as number and type of wireline outlets or satellite dishes, set-top boxes, and remote controls. In addition, transactional data will be collected whenever individuals select specific video programs that are billed separately, as in pay-per-view programs. This may include the video program selected, the date, and time.

Thus, a great deal of information is collected currently by both telephony and video service providers. However, because of differences in the way that those markets developed and the way in which they were regulated, the regulations and policies governing the accumulation and use of such information vary among markets and, frequently, among firms competing in the same market. The following discussion highlights that variety and outlines some of the problems that it creates for safeguarding personal information privacy, now and in the future.

B. Existing Privacy Protections Pertaining to Telephony Services

In addition to government regulations concerning the acquisition, disclosure, and use of TRPI by telephone service providers, many of those companies have long-standing internal policies to safeguard customer privacy.[41] These policies generally make one restriction clear: calling records shall not be disclosed to third parties. For example, BellSouth stated in its comments that it does not provide unauthorized third parties access to consumer toll records or accounts.[42] A few telephone companies have recently developed more formal privacy codes that specifically inform residential customers about company information practices and options for limiting access to personal information. For example, Pacific Bell indicated that its privacy guidelines allow customers to prohibit information collected about them to be used for marketing purposes.[43] Bell Atlantic's residential customer information privacy principles include disclosure

41 *See* Comments of GTE at 3; Comments of Bellsouth at 14-16; Comments of Bell Atlantic at 4; Comments of AT&T at 6; Comments of Southwestern Bell at 5; Comments of U S West at 3; Letter from Gerald J. Kovach, Senior Vice President, External Affairs, MCI, to Chairman Edward Markey, House Subcommittee on Telecommunications and Finance (May 20, 1992), (on file at NTIA).

42 *See* Comments of BellSouth at 14-15; *see also* Comments of U S West at 16 (stating that transactional data is not released without customer consent); Letter from Gerald J. Kovach, Senior Vice President, External Affairs, MCI, to Chairman Edward Markey, House Subcommittee on Telecommunications and Finance (May 20, 1992) (on file at NTIA) (noting that MCI does not sell or rent its customer lists or information about customers to third parties).

43 *See* Pacific Bell, *Customer Privacy Guidelines* (Sept. 1993) (brochure).

policies regarding how personal information is collected and used.[44] In September 1995, MCI announced that online internetMCI customers could call a toll free 800 number to prevent personal information about themselves from being included in on-line directories or made available to third parties.[45]

There is evidence, however, that the privacy policies of telephone companies may not always be followed. For example, it appears that private investigators regularly obtain calling records. As reported in the Wall Street Journal:

> *Although most phone companies say they won't release information unless they are subpoenaed, the information is released on an informal basis all the time, says Mr. [Robert Ellis] Smith, of Privacy Journal. He says most such releases are arranged by law-enforcement officials who have relationships with telephone-company employees.*[46]

In another well known example, an Alaskan oil pipeline company hired a private security firm to obtain the calling records of its critics.[47] During a subsequent investigation, a former state prosecutor testified at the hearings that telephone companies routinely provide calling records to contractors, with knowledge that the records will be sold to private investigators.[48] In fact, companies specializing in calling records target advertisements to private investigators.[49]

As for government action, the FCC has established regulations governing the use and disclosure of customer proprietary network information (CPNI).[50] CPNI is essentially TRPI that

---

44 These principles also commit Bell Atlantic to evaluating "potential privacy impacts" associated with providing interactive multimedia services. *See* Bell Atlantic Network Services, Inc., *Residential Customers Information Privacy Principles* (Jan. 1995) (brochure).

45 *See* Consumer Affairs, MCI Telecommunications, *MCI Telecommunications Information Privacy Policy* (Sept. 1995).

46 Bruce Knecht, *A New Casualty in Legal Battles: Your Privacy*, Wall St. J., Apr. 11, 1995, at B1.

47 *See Telephone Privacy: Hearings Before the Subcomm. on Telecommunications and Finance of the Comm. on Energy and Finance, House of Representatives*, 103d Cong., 1st Sess., 4-5 (1993) (statement of Hon. George Miller, Cal.) [hereinafter Miller Statement]; *see also* S.T. Parker, *Alyeska "Spy" Witness Heard By House Panel; Committee on Interior and Insular Affairs*, Oil Daily, Nov. 5, 1994, at 1.

48 *See Miller Statement, supra* note 46, at 7.

49 *See* L. Morgan and E. Wilson, *Anyone Can See Your Toll Charges*, St. Petersburg Times, Oct. 1, 1993, at 1B.

50 A number of States have adopted laws and regulations regarding disclosure of CPNI, which generally apply only to intrastate telephone services. For example, California prohibits disclosure of calling records to third parties, without the subscriber's prior written authorization. In addition, California also prohibits telephone or telegraph corporations from disclosing the "services which the residential subscriber purchases from the corporation or from independent suppliers of information services who use the corporation's telephone or telegraph line to provide service to the residential subscriber." *See* Cal. Pub. Util. Code sec. 2891 (1995). Similarly, New York and Hawaii adopted privacy provisions covering telephone subscriber information in 1994 and 1995. *Sector Reports: Telecommunications*, Privacy & Am. Bus., May/June 1995, at 21.

is collected in providing telephony services and "encompasses any information about customers' network services and their use of those services that a telephone company possesses because it provides those network services."[51] CPNI includes "information related to the type(s), location(s), and quantity of all services to which a customer subscribes, how much the customer uses them, and the customer's billing records."[52] These requirements only apply to interstate services.

The Commission's CPNI rules were not specifically implemented to address privacy concerns.[53] The primary consideration was that if dominant service providers had detailed information about customers' basic service requirements, this information could be used to gain an anticompetitive advantage in unregulated markets, specifically the enhanced service and customer premises equipment markets. Consequently, the rules only apply to a limited number of companies—the Bell companies,[54] and GTE—and do not protect the CPNI of all customers.[55]

Under the CPNI rules, if a customer requests confidential treatment of CPNI, the Bell companies and GTE must not disclose this information to their affiliates or to third parties. If no confidentiality request is made, then the rules vary about the type of protection that the data is accorded.[56] The Bell companies and GTE are required to notify only multi-line customers of the right to request confidential treatment of CPNI. Single-line and residential customers need not be notified, and no prior authorization is required before using the CPNI of these customers for marketing or other purposes ancillary to the provision of telephone service.

---

51 *See Additional Comment Sought on Rules Governing Telephone Companies' Use of Customer Proprietary Network Information,* Public Notice, 9 FCC Rcd 1685 (1994) *citing Filing and Review of Open Network Architecture Plans,* 4 FCC Rcd 1, ¶ 403 (1988) [hereinafter *ONA Plans].*

52 *ONA Plans* (noting general description given by NYNEX). The FCC clarifies that CPNI does not, however, include credit information. *Id.* ¶412.

53 The FCC has consistently stated over the years that its CPNI rules are "intended to balance considerations of efficiency, competitive equity, and privacy." *Computer III Remand Proceedings: Bell Operating Companies Safeguards and Tier I Local Exchange Carriers,* 6 FCC Rcd 7571, ¶ 84 (1991) [hereinafter *BOC Safeguards Order].*

54 The term "Bell companies" as used here refers to the seven Regional Holding Companies formed as part of the divestiture of AT&T in 1984, and their operating subsidiaries.

55 These rules also applied to AT&T until recently. On October 12, 1995, the FCC reclassified AT&T as a non-dominant interexchange carrier. This decision frees AT&T from regulations such as the CPNI rules that apply specifically to dominant carriers. *See Commission Declares AT&T Non-dominant,* FCC Press Release No. 95-60, Common Carrier Action (Oct. 12, 1995).

56 *BOC Safeguards Order, supra* note 53, pt. III.C. For example, the FCC requires the Bell companies and GTE to obtain the prior authorization of customers with twenty lines or more before disclosing the CPNI of these customers to enhanced service provider (ESP) affiliates. No prior authorization is required for customers with fewer than twenty lines, nor is any prior authorization required—regardless of the number of customer lines—for CPNI disclosures to Bell companies and GTE customer premises equipment affiliates. *Id.* at ¶ 89.

More significantly, there are no FCC prohibitions on the disclosure and use of CPNI by more than one thousand independent local exchange carriers, non-wireline cellular carriers, interexchange carriers, competitive access providers, or other businesses engaged in the provision of telecommunications services. Similarly, the FCC's CPNI rules currently would not apply to traditional cable operators when they begin to provide telephone service.

C. Current Privacy Protections Pertaining to Video Services

Unlike telephone service providers, video carriage service providers[57] can play a dual role, providing both programming and the transmission service necessary to reach their customers. Although cable television service is the most widely known video carriage service, many telephone companies have announced plans to provide video carriage through wire-based telephone networks adapted to transmit video content. Moreover, a growing number of firms are offering video programming services using wireless technologies such as direct broadcast satellites (DBS) and "wireless cable" services.[58]

The privacy concerns associated with video carriage are similar to those concerns that prompted passage of the Video Privacy Act of 1988 (Video Act). During Judge Robert Bork's Supreme Court nomination hearings, 146 video titles rented by him and his family were disclosed to the press.[59] Congressional testimony revealed that Judge Bork's case was not isolated. Various examples of demands for video transactional records were mentioned, including an attempt to use video tape records to show that a spouse was an unfit parent, and a defendant in a child molestation case who wanted to show that the child's accusations were based on movies viewed at home.[60]

The Video Act prohibits video tape service providers from knowingly disclosing personal information, such as titles of video cassettes rented or purchased, without the individual's written consent.[61] It permits disclosure of mailing list information (names and addresses) if the

---

57 For this discussion, "video carriage" includes all communications services that transmit television-like content through wireline and wireless technologies.

58 Of course, television broadcasts also transmit video programming. There have been no privacy concerns, however, associated with this communications service because so far TRPI has not been collected about an individual's television viewing patterns—except for those cases in which an individual agrees to record his or her viewing for a survey company in exchange for consideration.

59 *See* Michael Decourcy Hinds, *Personal But Not Confidential: A New Debate Over Privacy*, N.Y. Times, Feb. 27, 1988, at 56.

60 *See Video and Library Privacy Protection Act of 1988: Joint Hearing on H.R. 4947 and S. 2361 Before the Subcomm. on Courts, Civil Liberties, and the Administration of Justice of the Senate Comm. on the Judiciary*, 100th Cong, 2d Sess. 80, 84 (1988) (testimony of Vans Stevenson for the Video Software Dealers Association and Erol's Inc.).

61 *See* 18 U.S.C. § 2710(b)(1) (1988).

individual has been given a conspicuous opportunity to prohibit such disclosure.[62] The mailing list can identify the subject matter (but not specific titles) of customer video selections, as long as that mailing list is used solely to market goods and services directly to the individual.[63] Finally, the Video Act requires personal information to be destroyed "as soon as practicable, but no later than one year from the date the information is no longer necessary for the purpose for which it was collected," provided that statutorily recognized requests for such information are not pending.[64]

Congress also acknowledged potential privacy concerns associated with delivering video programming over cable networks when it included subscriber privacy provisions in the Cable Communications Policy Act of 1984 (Cable Act). The Cable Act requires cable operators to notify subscribers at the time of subscription and, at least annually thereafter, of the operator's personal information practices.[65] Absent a subscriber's prior written or electronic consent, the Act allows a cable operator to collect personal information only if it is necessary to render the requested services or to detect unauthorized reception of cable communications.[66] Further, the Cable Act generally prohibits the disclosure of personal information unless such disclosure is necessary to render the services requested or to a "legitimate business activity related to" such service.[67] With few exceptions, any other collection or disclosure of personal information requires prior consent by the individual.[68] Finally, the Cable Act requires personal information

---

62 *See id.* § 2710(b)(2)(D)(i). Disclosures "incident to the ordinary course of business of the video tape service provider" are also permitted. *Id.* § 2710(b)(2)(E).

63 *See id.* § 2710(b)(2)(D)(ii).

64 *Id.* § 2710(e). The Video Act also has specific provisions governing governmental access to video tape records, *see id.* § 2710(b)(2)(C), as well as court ordered requests in a civil proceeding, *id.* § 2710(b)(2)(F). States have passed similar video tape laws. *See, e.g.*, Cal. Civ. Code § 1799.3 (West 1995); Del. Code Ann. tit. 11, § 925 (1994).

65 *See* 47 U.S.C. § 551(a) (1988 & Supp. V 1993). Among other things, such notice must state the nature of the personal information collected and its use; the nature, frequency, and purpose of disclosures; the length of time the information is kept; times and places where the subscriber may have access to the stored information; the legal limitations of the service operator; and the enforcement rights of the subscriber. *See id.* Federal case law has established a sufficiency test for notice similar to that used in a Truth In Lending Act analysis. *See Scofield v. Telecable of Overland Park, Inc.*, 973 F.2d 874, 879 (10th Cir. 1992). "Clear and conspicuous" notice (as required under the Cable Act) must provide "meaningful disclosure" which is essentially "warn[ing] an ordinary subscriber of practices that materially affect his privacy interests." *Id.* at 880. Perfect disclosure is not required, rather, only that which is reasonable. *Id.*

66 *See* 47 U.S.C § 551(b)(2) (1988).

67 *Id.* § 551(c)(2)(A).

68 *See id.* §§ 551(b)(1), 551(c)(1) (1988 & Supp. V 1993). The exceptions include disclosure of information pursuant to a court order, *see id.* §§ 551(c)(2)(B), 551(h); disclosure of mailing list information (names and addresses) if the individual had a prior opportunity to prohibit such disclosures, *see id.* § 551(c)(2)(C)(i); *and* the disclosure that does not reveal, even indirectly, the subscriber's viewing habits or use of the service *or* any nature of a subscriber's transactions over the service. *Id.* § 551(c)(2)(C)(ii).

to be destroyed if the information is no longer necessary for the purpose for which it was collected and if there are no legally recognized, pending requests for such information.[69]

A review of the Video Act reveals that it may not be applicable to consumers of video services provided over telecommunications networks. This is because the Video Act was intended to cover the traditional rental, sale or delivery of video cassette tapes or similar material from a video store.[70] It therefore may be argued that because video carriage does not involve a delivery of a physical tape or similar material to the individual, and is instead transmitted electromagnetically through wireline or wireless facilities, the Video Act does not apply to video programming transmitted through telecommunications networks.[71]

While the Cable Act obviously applies to video carriage provided by cable operators, it does not expressly apply to video carriage by DBS or wireless cable service operators.[72] Moreover, it is uncertain whether it will apply to LEC provision of video programming. This question turns on whether LECs are deemed "cable operators" within the meaning of the Cable Act. If LECs operate under a purely common carrier VDT model, they may not be considered cable operators.[73] On the other hand, if LECs operate in a manner similar to cable operators—then

---

69 *See id.* § 551(e) (1988). States have passed similar cable privacy laws. *See, e.g.*, Cal. Penal Code § 637.5 (1995); Conn. Gen. Stat. Ann. § 53-421 (1994); Ill. Ann. Stat. ch. 38, para. 87-2 (1995); and Wisc. Stat. Ann. § 134.43 (1994).

70 Furthermore, it is not clear whether video carriage providers could be considered "video tape service providers" within the meaning of the statute. The Act defines "video tape service providers" as any person engaged in the "rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual materials." 18 U.S.C. § 2710(a)(4) (1988).

71 Commenters to the Privacy NOI concurred with this interpretation. *See, e.g.*, Comments of Time Warner at 11; Comments of Bell Atlantic at 8; Comments of Southwestern Bell at 12-13; Comments of AT&T at 13-14.

Although commenters argued that the Video Act does not apply to service providers that distribute video over telecommunications networks, some recommended that similar privacy provisions be applied to such services since there is little difference between renting a video from a store and ordering to view it over a communications network. *See* Comments of MCI at 12-13; Comments of National Cable Television Association at 5-6.

72 *See Definition of a Cable Television System*, 5 FCC Rcd 7638, 7638 (1990) ("[T]he term cable system as used in the [Cable] Act encompasses only video delivery systems that employ cable, wire, or other physically closed or shielded transmission paths . . . . [D]irect broadcast satellites and so-called 'wireless cable' . . . are not cable systems.").

73 *See NCTA v. FCC*, 33 F.3d 66, 71 (1994). To be a "cable operator," an entity must engage in the "transmission" of video programming. *See* 47 U.S.C. §§ 522 (5),(6) (1988). In *NCTA*, the court upheld the FCC's determination that "transmission" requires "active participation in the selection and distribution of video programming." *NCTA*, 33 F. 3d at 71, 73 (quoting FCC Order). LECs serving purely as common carrier conduits would thus not be transmitting programming.

Although LECs providing video programming might not be subject to the Cable Act's subscriber privacy provision, GTE and the Bell companies would still be subject to the FCC's CPNI rules. *See Telephone Company-Cable Television Cross-Ownership Rules, Sections 63.54-63.58* 10 FCC Rcd 244 ¶ 239 (1994).

they may be deemed cable operators.[74] In absence of other privacy provisions regarding personal information generated as a result of subscribing to video services electronically, consumers of seemingly like video services may or may not receive disparate levels of protection, while providers of these services may or may not be subject to different regulatory requirements.

D. Lack of Uniformity

This brief review of TRPI disclosure protections relating to telephony and video carriage services reveals the lack of *intra*service uniformity: like services do not have like privacy protection. With respect to telephony services, for example, Federal regulations grant individuals the right to ask for confidential treatment of CPNI but only from certain telephone companies—the Bell companies and GTE. Similarly, the notice requirements that apply to the Bell companies and GTE differ depending on the type of consumer. Multi-line customers are given notice about their privacy rights; single-line customers are not. To complicate matters further, a few states provide privacy protection for intrastate service regardless of which telephone company is involved.

There is also a lack of intraservice uniformity for video carriage. The privacy provisions of the Cable Act do not apply to DBS and wireless cable operations. And it is not clear whether the Cable Act applies to LECs that operate as video service providers—although from a consumer's perspective, such services are functionally indistinguishable.

In addition, there is a lack of *inter*service uniformity because like-types of information are not treated in like-ways, across different communications services. Many other types of communications services that generate TRPI, as sensitive as TRPI generated by telephone service and video carriage, are almost entirely unprotected. For example, the Internet, a global network of networks, which can be used for interactive, point-to-multi-point communications, is not subject to consumer privacy regulations. Internet access is provided by dedicated Internet service providers (ISPs) or on-line services that have gateways to the Internet.[75] Depending on the particular technological configuration, the ISP may have TRPI in the form of "calling" records (*e.g.*, what Internet Protocol address communicated with whom and when), transactional records

74 In comments to the FCC, NTIA has argued that when a LEC offers video programming via a VDT platform, the LEC should not be deemed a "cable operator." *See* Comments of NTIA *in* CC Docket No. 87-266, at 22-28 (filed July 11, 1995).

75 As of 1994, approximately 300 regional and national ISPs offered individuals access to the Internet at various levels. ISPs can provide dedicated access, which may involve leasing a dedicated telephone line and installing an Internet routing computer at the individual's site. ISPs can provide software that allows individuals to connect their home computers to office, university, or private time-sharing networks that have dedicated access to the Internet. In addition, many on-line services, which principally provide information products and discussion fora to subscribers, have gateways to communicate via the Internet. The distinction between ISPs and on-line services is dissolving as ISPs provide more information products and as on-line services provide less restricted access to the Internet through their gateways. *See* Ed Krol, *The Whole Internet* 456-66 (2d ed. 1994).

of files uploaded or downloaded, and electronic mail messages sent and received.[76] Besides the Electronic Communications Privacy Act of 1986 (ECPA), which forbids only divulging the *contents* of a communication, no federal privacy laws apply to TRPI collected by those who provide Internet access.[77]

On the horizon are a new generation of communications services that will combine the two-way, switched features of telephone service, the full interactivity of the Internet, and the broadband capacity of video carriage. LECs planning to carry video may expand their facilities to include fully two-way interactive video traffic.[78] Traditional cable operators are restructuring their service platforms with fiber-optic trunk lines, data compression, and high speed switching

---

76 For example, CompuServe sells mailing lists to third-parties "broadly based on member segments or selections," *Communications Daily*, Oct. 25, 1994, at 3 (electronic version), making available "interest categories which represent the on-line use of CompuServe members." *Id.* (quoting Direct Media, list-compiler). Similarly, America Online sells personal information about its subscribers: name, address, [and] *type of customer*. *Communications Daily*, Oct. 26, 1994, at 4 (electronic version) (emphasis added). Both America Online and CompuServe allow individuals to opt-out of such mailing lists. *See* text at Part III (analyzing opt-in and opt-out schemes).

In contrast, Prodigy has a policy of not disclosing any personal information about its subscribers to third-parties. Prodigy Services Co., *Policy on Protecting Member Privacy* (on file at NTIA). In addition, Apple Computer, Inc. (AppleLink, Eworld), Delphi Internet Services Corp., New York Times Service/Syndication, ProductView Interactive, and Dow Jones & Co., Inc., have internal policies prohibiting release of personal information to third parties. *See Communications Daily*, Oct. 26, 1994 (electronic version).

77 18 U.S.C. § 2511(3)(a) (1988). The ECPA forbids a provider of "electronic communication service to the public" to "intentionally divulge the contents of any communication . . . while in transmission on that service" to any unauthorized entity. *Id.* The term contents "includes any information concerning the substance, purport, or meaning of that communication." The ECPA, however, makes clear that "contents" do not include "the identity of the parties or the existence of the communication." § 2510 (8). The ECPA allows providers to "disclose a *record* or other *information pertaining to a subscriber* . . . not including the *contents* of communications" to any nongovernmental entity. *See* 18 U.S.C. § 2703(c)(1)(A) (1988) (emphasis added). The ECPA does not explicitly define "record" and, to date, no court has interpreted this term. Thus, it is an unsettled question of law whether information, such as the subject line of an e-mail message or the title of video programming viewed, qualifies as "content" or merely as a transactional "record."

A strong argument may be made that by transaction records, Congress meant nothing more than information that reveals the origin, destination, and existence of a communication. The legislative history of the ECPA reveals that transactional records were left out of the definition of contents in order to harmonize the statute with Fourth Amendment jurisprudence that left calling record information unprotected. *See* S. Rep. No. 541, 99th Cong., 2d Sess., 13 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3567. ("The Supreme Court has clearly indicated that the use of pen registers, *i.e.* calling records associated with telephone service, does not violate either chapter 119 of title 18 or the fourth amendment. [This section] of this legislation makes that policy clear."). *See also* Office of Enforcement Operations, Criminal Division, U.S. Dep't of Justice, *Analysis of the Electronic Communications Privacy Act of 1986, Public Law No. 99-508* (Dec. 15, 1986) ("In electronic communications [transactional records] are the records that are the equivalent of the traditional telephone toll records maintained by a telephone company."). Based on this interpretation, from a privacy point-of-view, there may be no meaningful difference between, for example, the contents of a communication and transactional data that identifies the title or the specific nature of the communication.

78 *See* Mark Berniker, *Bells Close Disney Video Services Deal*, Broadcasting & Cable, Apr. 24, 1995, at 34.

to provide interactive multimedia communications.[79] Importantly, convergence will occur not only between technologies, firms, and services, but also between functions so that communications providers will become content providers and vice-versa. As these new communications services become widely available, providers will have access to greater amounts of more sensitive TRPI. Of course, one cannot know precisely what sorts of TRPI will be collected because these new communications services are not fully designed, much less fully operational. It is also uncertain which, if any, privacy protections will apply to such new services. For example, it is uncertain whether the Cable Act could apply to these new interactive broadband networks because truly interactive services may not be deemed a "cable service" within the meaning of the Act.[80]

III. PROPOSED FRAMEWORK FOR COLLECTION AND USE OF TRPI

The limitations and weaknesses in the telecommunications privacy regulations discussed above underscore the need for a more comprehensive approach governing the collection, use, and dissemination of TRPI by providers of telecommunications and information services. Of course, any such approach must recognize that information privacy can never be absolute in a sociological setting: no individual who lives in a society can have total control over each bit of personal information. In fact, as various commenters pointed out, the free exchange of personal information promotes consumer welfare by encouraging firms to develop and market the goods

79 Many cable operators are currently restructuring their networks to deliver a variety of services. These services range from traditional one-way multi-channel video programming to telephony, to higher-speed access to remote databases, and using these networks as the backbone for various wireless services. *See* Interview with Amos Hostetter, Chairman/CEO of Continental Cablevision, *The Once and Future Cable,* Broadcasting and Cable, May 8, 1995, at 33.

In October 1994, Time Warner introduced the first switched, digital interactive, multimedia network, called the Full Service Network (FSN) in Orlando, Florida. An existing coaxial cable network in Orlando was upgraded with fiber-optic technology to develop this FSN. In addition, high capacity multi-access digital storage systems-servers were added to facilitate the transactions of multiple customers simultaneously, and a form of high speed switching called asynchronous transfer mode (ATM) technology was added to route digital, video, voice, or computer data from digital libraries to individual homes. Eventually, Time Warner hopes to use this network to bring a host of services to consumers' homes including: access to libraries, distance learning, news-on-demand, long distance telephone access, banking and other financial services, driver's license renewal or tag registration, grocery and drugstore shopping, medical imaging, high-speed data transport for business, video conferencing, HBO-on-demand, sports-on-demand, and music-on-demand. Time Warner Cable, Full Service Network, *Background: Time Warner Introduces World's First Full Service Network in Orlando* (May 1995).

80 Cable service refers to video programming similar to current television broadcasts. *See* 47 U.S.C. § 522(6)(a)(b) (1988). Limited subscriber interaction is included in "cable service," but only to the extent of selecting video programming from a menu typical of pay-per-view. Interactive multimedia services may not be considered a "cable service" because they do not resemble today's one-way video programming and involve a high level of subscriber interactivity.

and services that most interest their existing and potential customers.[81] On the other hand, the new information environment may promote the acquisition and use of personal information in ways that violate deeply held societal values about confidentiality and fairness.

The Administration recognizes that, in some circumstances, "an individual's privacy can often be best respected when individuals and information users come to some mutually agreeable understanding of how personal information will be acquired, disclosed, and used."[82] Under this "contractual approach" to privacy protection, companies would inform their customers about what sorts of personal information the firms intend to collect and the uses to which that information would be put. Consumers could then either accept a company's "offer," or reject it and shop around for a better deal. The contractual approach reflects the hope that individuals and the parties with whom they do business can agree, in whatever form the agreements may be made, about how TRPI and other personal information will be acquired, disclosed, and used —all without substantial involvement by the government as referee. Rather than relying on the government to determine what information should be protected, consumers and service providers could decide among themselves what is the optimal level of privacy protection. In this way, the contractual approach seeks to minimize government involvement in assessing and resolving privacy problems.

Nevertheless, although the contractual approach has many virtues in theory, it may not provide a sufficient level of privacy protection in practice. That approach yields maximum benefit in a vigorous competitive marketplace, where privacy is one of the terms on which businesses struggle for customers and where consumers can walk away from transactions that do not provide adequate privacy protection, secure in the knowledge that other offers will be readily available. In contrast, in markets where essential or highly desired services are provided by a single firm or a small group of dominant firms—such as the local telephone and video service markets—competition on privacy will be, at best, weak and consumers will not be able to reject or renegotiate unacceptable privacy "offers." In other circumstances, a contractual approach could produce instances where service providers offer privacy protection only at a premium, to the detriment of poor and low income consumers.

For these reasons, NTIA does not support adoption of a "pure" contractual approach. Rather, we favor a modified contractual model that allows businesses and consumers to reach agreements concerning the collection, use, and dissemination of TRPI, subject to two fundamental requirements—provider notice and customer consent. Our recommended approach should adequately protect individuals' legitimate privacy interests without excessive government intervention in the marketplace. Further, by giving consumers effective controls over the use of TRPI generated by their subscription to and use of the NII, that approach should expand consumer demand for NII facilities and services. That, as noted above, should produce

---

81 "Presently, more than 111 million Americans rely upon the convenience and diversity of products when shopping by phone or mail. Because of direct response marketing, consumers can select from thousands of essential, hard-to-find products and services in the comfort of their living rooms." Comments of the Direct Marketing Association at 4.

82 *IITF Principles, supra* note 11, at Commentary ¶ 4.